Remarks

These Remarks are in reply to the Final Office Action mailed October 6, 2008, and are being filed concurrently with a REQUEST FOR CONTINUED EXAMINATION UNDER 37 C.F.R. §1.114.

I. Summary of Examiner's Rejections

Prior to the Final Office Action mailed October 6, 2008, Claims 1-12 and 14-30 were pending in the Application. In the Office Action, Claims 1-12 and 14-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hanna et al. (U.S. Patent No. 7,054,905) in view of Arnold (U.S. Patent No. 6,275,848) and Le Pennec et al. (U.S. Publication No. 2005/0076082).

II. Summary of Applicants' Amendment

The present Response amends Claims 1, 5, 12 and 19, leaving for the Examiner's present consideration 1-12 and 14-30. Reconsideration of the Application, as amended, is respectfully requested.

III. Claim Rejections under 35 U.S.C. §103(a)

In the Final Office Action mailed October 6, 2008, Claims 1-12 and 14-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hanna et al. (U.S. Patent No. 7,054,905, hereinafter Hanna) in view of Arnold (U.S. Patent No. 6,275,848, hereinafter Arnold) and Le Pennec et al. (U.S. Publication No. 2005/0076082, hereinafter Le Pennec).

Claim 1

Claim 1 has been amended to more clearly define the embodiment therein. As amended, Claim 1 defines:

> *1. A method for processing electronic mail messages, the method comprising:*
> *accepting an electronic mail message, the electronic mail message including a file attachment;*
> *removing the file attachment from the electronic mail message;*
> *storing the file attachment in an attachment location;*

inserting a hyperlink in the message, the hyperlink associated with the attachment location, wherein the hyperlink causes submission of validation information to an attachment server storing the file attachment;

embedding a security token into the electronic mail message, wherein the security token specifies a security credential that would be transmitted to the attachment server when said hyperlink is utilized by a browser;

receiving a retrieval request from a recipient of the electronic mail message; and

determining, based on the security token embedded in the electronic mail message, whether to allow access to the attachment by the recipient and allowing access to the attachment if said security credential is deemed acceptable; and

performing transduction on the file attachment by the attachment server prior to providing the file attachment to the recipient, wherein transduction is performed by the attachment server modifying a format of said attachment into a different format that enables the recipient to access the attachment, streaming the attachment to said recipient or translating text contained in said attachment.

As amended, Claim 1 defines a method for securely distributing email attachments and performing transduction on the attachments before providing them to a recipient. More specifically, at the time of sending an email message, the attachment is removed from the email and stored on the attachment server. A security token is then embedded into the message, along with a hyperlink to the attachment server. The security token specifies a security credential (e.g. a password) that would be transmitted to the attachment when the hyperlink is utilized by a browser. In other words, the modified email message now contains security information for accessing the attachment which was removed from that message.

After the message is sent, a request to retrieve the attachment is received from the recipient. At this point, the attachment server can determine, based on the previously embedded security token, whether to allow access to the recipient.

In addition, the attachment server performs transduction on the attachment. The transduction is performed before access to the attachment has been provided to the recipient. Specifically, transduction includes the attachment server modifying the format of the attachment to a different format that is accessible by the recipient, streaming the attachment to the recipient, and/or translating the text contained in the recipient.

Hanna teaches a method for replacing an email attachment with an address specifying where the attachment is stored. More specifically, Hanna describes a system that examines an email message to determine if the email contains an attachment. If the email does contain an

attachment, the system stores the attachment at a location on the network. The email message is modified by replacing the attachment with a reference specifying its location. The email is then sent to the recipient and the recipient uses the reference to retrieve the attachment (col. 2, lines 1-19).

Arnold teaches automated referencing of electronic information. More specifically, Arnold was cited as disclosing applying detachment rules to the email message. These "detachment rules include criteria for determining whether or not the attachment should be detached from the message… The criteria may include message size, number of recipients, type of recipient… and other configurable factors" (Arnold, col. 4, lines 9-17).

Le Pennec teaches managing the exchange of files attached to electronic emails. More specifically, Le Pennec was cited as disclosing the ability to encrypt and/or compress an original file sent via FTP or HTTP protocol (Le Pennec, par. [0029], [0061]).

However, Applicant respectfully submits that Hanna in combination with Arnold and Le Pennec (the cited references) fail to render obvious the features of Claim 1, as amended.

To begin with, the cited references fail to disclose the step of *performing transduction on the attachment prior to providing the file attachment to the recipient, wherein transduction is performed by the attachment server modifying a format of said attachment into a different format that enables the recipient to access the attachment, streaming the attachment to said recipient if the attachment is a media file, or translating text contained in said attachment*, as defined in amended Claim 1. This type of transduction is not disclosed in any of the cited references. In the Office Action, it was proposed that Le Pennec teaches a method of performing transduction on the file attachment in paragraphs 29 and 61 (Office Action, page 4). However, these cited portions of Le Pennec merely describe an ability to encrypt or compress files when sending the file via FTP/HTTP. In contrast, Claim 1 has been amended to specifically define that transduction on the email attachment is performed by modifying the format of the attachment into a different format that enables the recipient to access it, or by streaming the attachment to the recipient, or by translating the text in the attachment. In contrast, Le Pennec merely discloses compression/encryption techniques for files transmitted over FTP. Applicant fully agrees with the Examiner that the general concepts of encrypting and compressing a file before sending it are well known in the art (e.g. Win Zip, etc.). However, what is not disclosed in Le Pennec, nor the other cited references, is the process of performing transduction on the email attachment before

the recipient receives the attachment by translating the attachment into formats the recipient can understand, or streaming the attachment, or translating the text.

Additionally, the cited references completely fail to disclose the step of *embedding a security token into the electronic mail message, wherein the security token specifies a security credential that would be transmitted to the attachment server when said hyperlink is utilized by a browser*, as defined in amended Claim 1. This feature places into the email message the security information (password) that will be used to access the attachment by the recipient of that message. No such embedding is performed in any of the cited references. Hanna does appear to contemplate the possibility of "authenticating the recipient to a computer system upon which the attachment is stored" (Hanna, col. 2, line 20-22). However, there is no disclosure of embedding the security token into the actual email message, which contained the attachment before it was removed, as defined in amended Claim 1.

In view of the above comments, Applicants respectfully submit that Claim 1, as amended, is neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

Claims 5, 12 and 19

Claims 5, 12 and 19, while independently patentable, recite limitations that, similarly to those described above with respect to Claim 1, are not taught, suggested nor otherwise rendered obvious by the cited references. Reconsideration thereof is respectfully requested.

Claims 2-4, 6-12, 14-18 and 20-30

Claims 2-4, 6-12, 14-18 and 20-30 are not addressed separately, but it is respectfully submitted that these claims are allowable as depending from an allowable independent claim, and further in view of the comments provided above. Applicants respectfully submit that Claims 2-4, 6-12, 14-18 and 20-30 are similarly neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

It is also submitted that these claims also add their own limitations which render them patentable in their own right. Applicants respectfully reserve the right to argue these limitations should it become necessary in the future.

IV. Conclusion

In view of the above remarks, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and reconsideration thereof is respectfully requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: January 6, 2009

By: /Justas Geringson/
Justas Geringson
Reg. No. 57,033

Customer No.: 23910
FLIESLER MEYER LLP
650 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 362-3800
Fax: (415) 362-2928